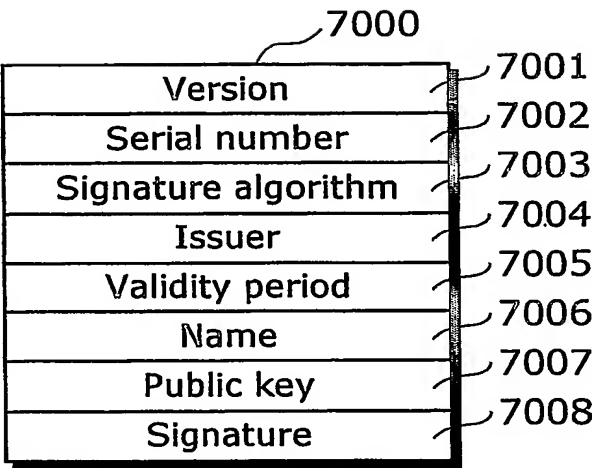


FIG. 2



The diagram shows a vertical stack of eight rectangular boxes, each representing a field in a data structure. A bracket on the left side of the stack is labeled '7000'. Each box contains a label, and a bracket on the right side of each box is labeled with a number from 7001 to 7008. The fields are: Version (7001), Serial number (7002), Signature algorithm (7003), Issuer (7004), Validity period (7005), Name (7006), Public key (7007), and Signature (7008).

Version	7001
Serial number	7002
Signature algorithm	7003
Issuer	7004
Validity period	7005
Name	7006
Public key	7007
Signature	7008

FIG. 3

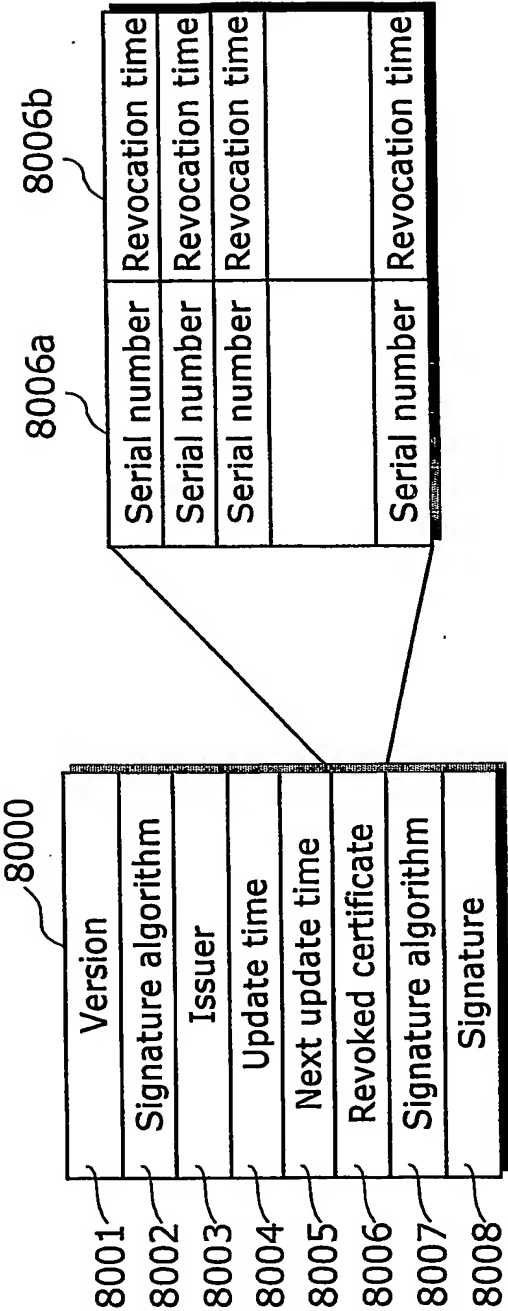
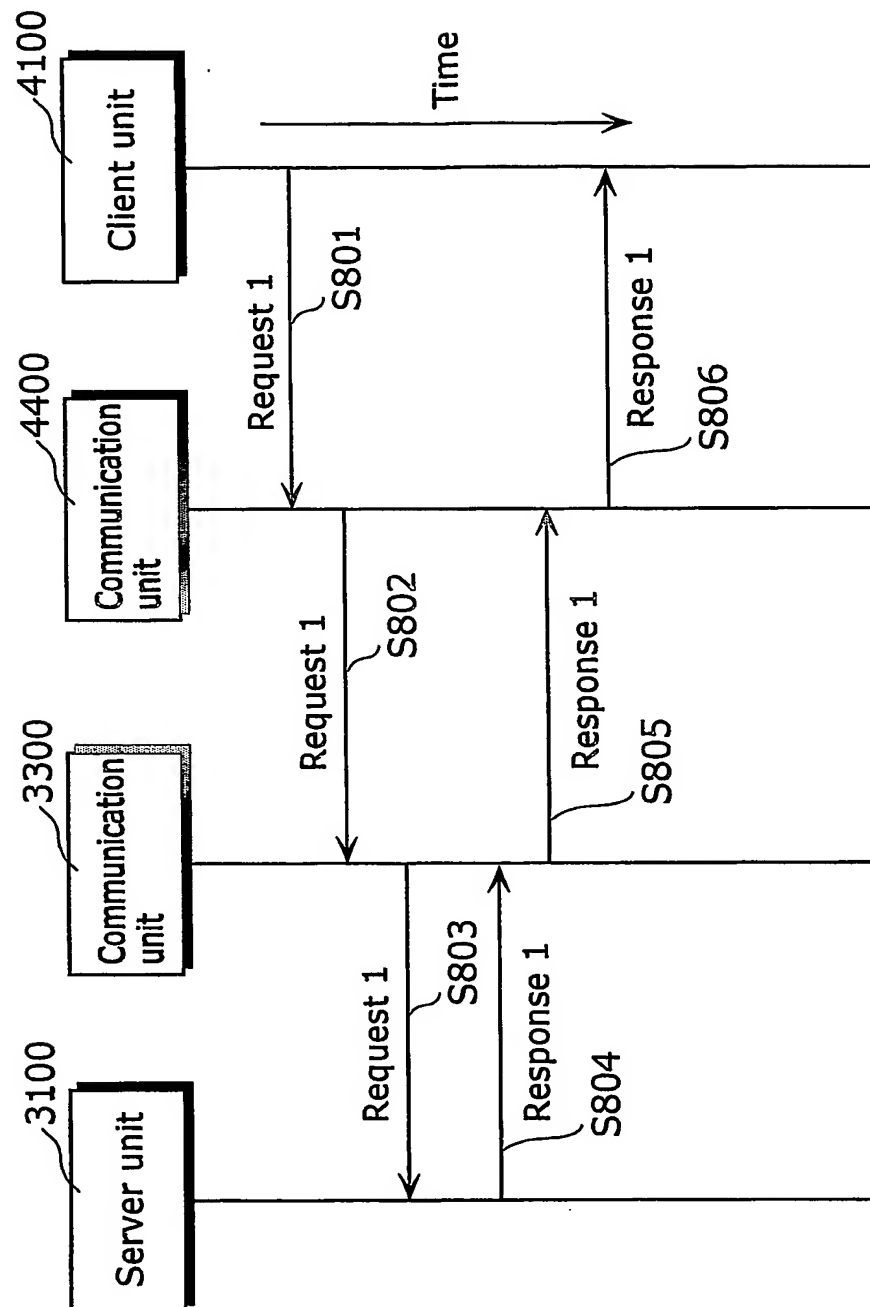


FIG. 4



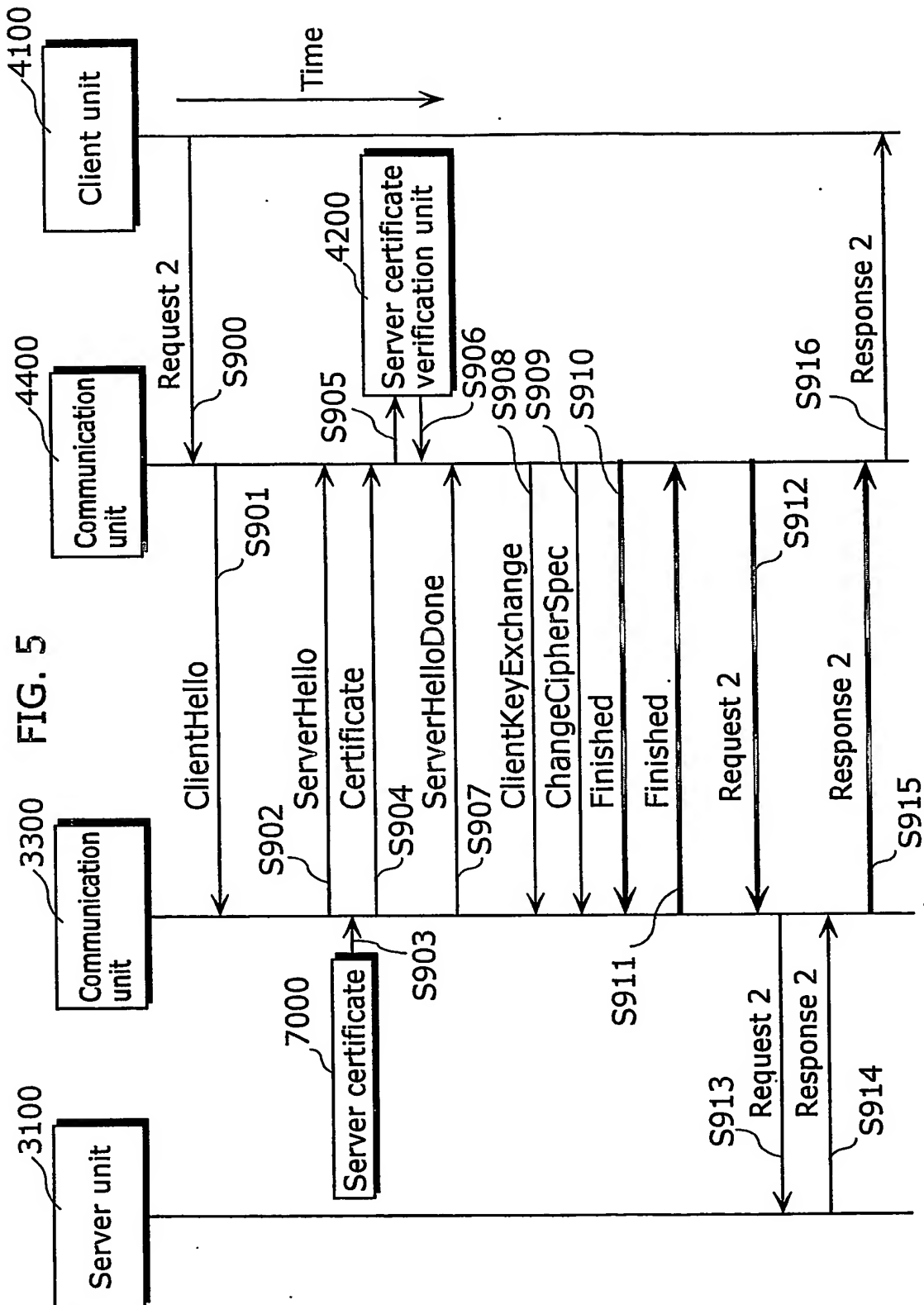
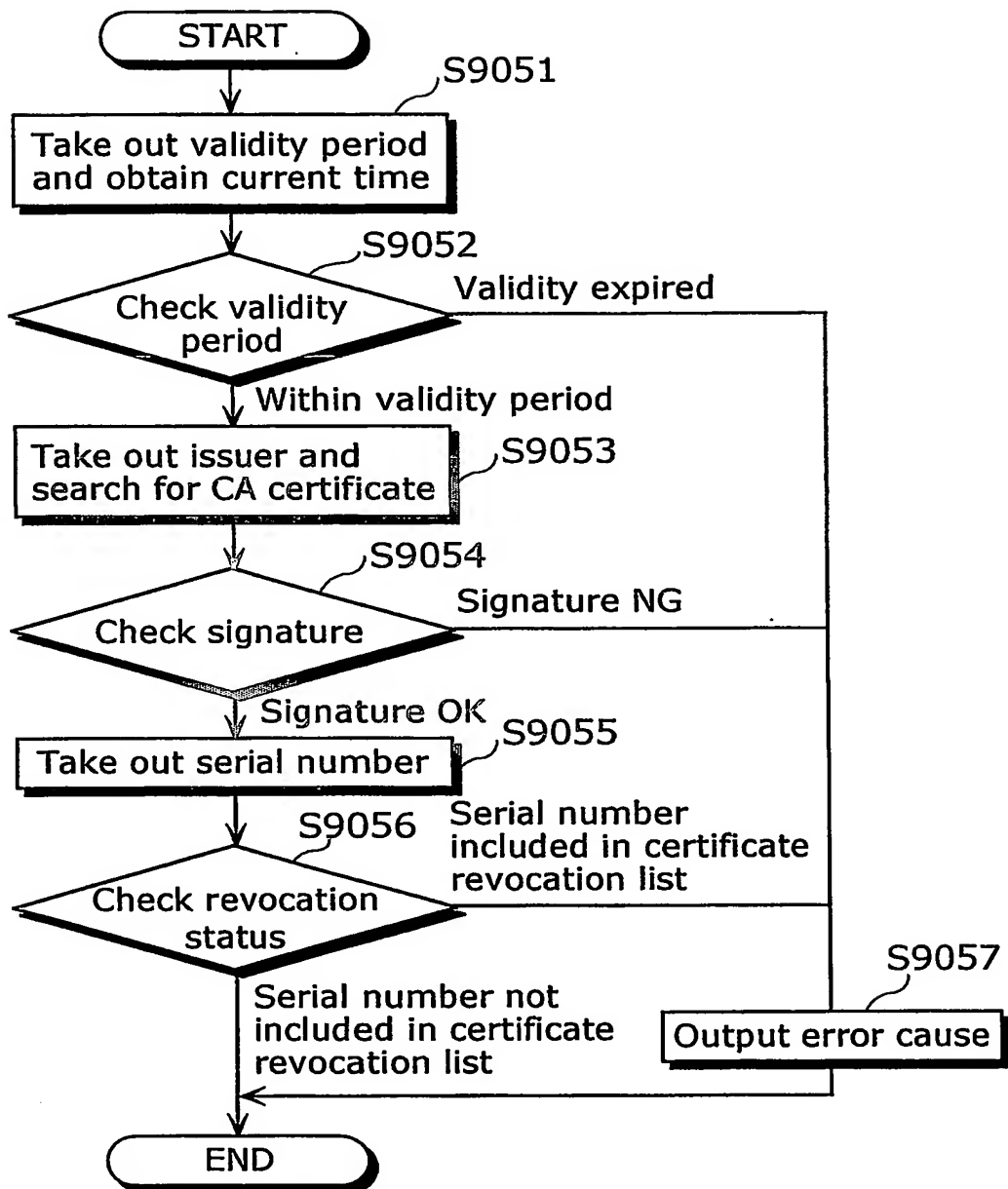


FIG. 6



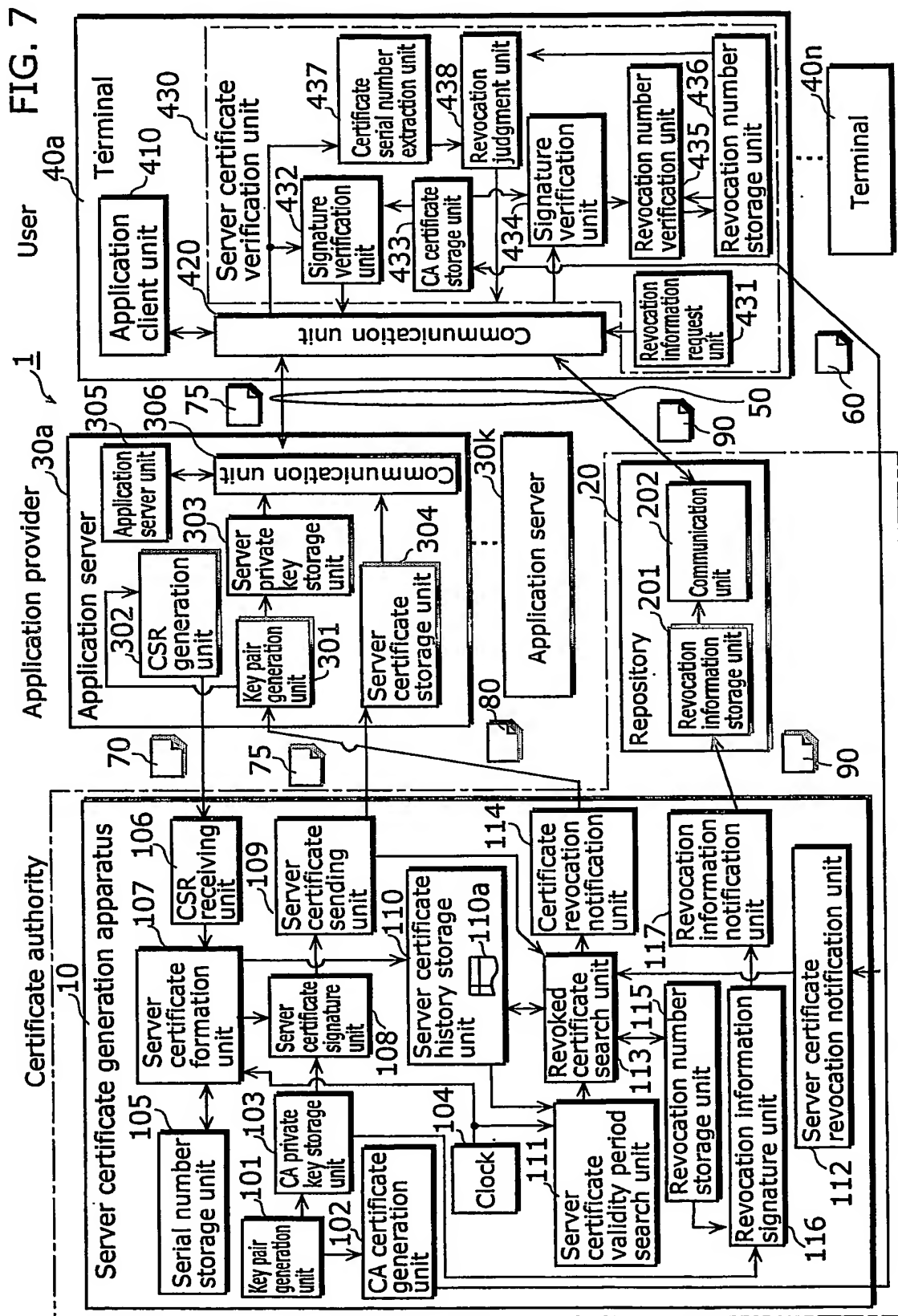


FIG. 8

## Server certificate 75

Version (1)	751
Serial number (17)	752
Signature algorithm	753
Issuer (Panasign)	754
Validity period (Start date/End date) (2003. 04. 01. 00. 00:…/ 2004. 05. 01. 00. 00:…)	755
Name (Hariwood movie)	756
Server public key (Pubk_11)	757
Signature (Sig(Seck_CA, Hariwood movie    Pubk_11))	758



FIG. 9

Revocation information 90

Issuer (Panasign)	91
Revocation number (0x0011)	92
Signature (Sig(Seck_CA, Panasign    0x0011))	93

FIG. 10

Server certificate history table 110a

1101		1102		1103
Server name	Server certificate serial number			Validity period
Hariwood movie	0x0011			2003.04.11.00.00:00.00
Big wave game	0x0012			2003.04.11.09.23:46.00
:	:			:
:	:			:
Robot trainer	0x0049			2003.11.03.09.23:46.00
Azalea recipe	0x0050			2003.11.11.12.51:51.18
:	:			:
:	:			:
Good drying day	0x0110			2004.05.10.21.42:35.00

FIG. 11

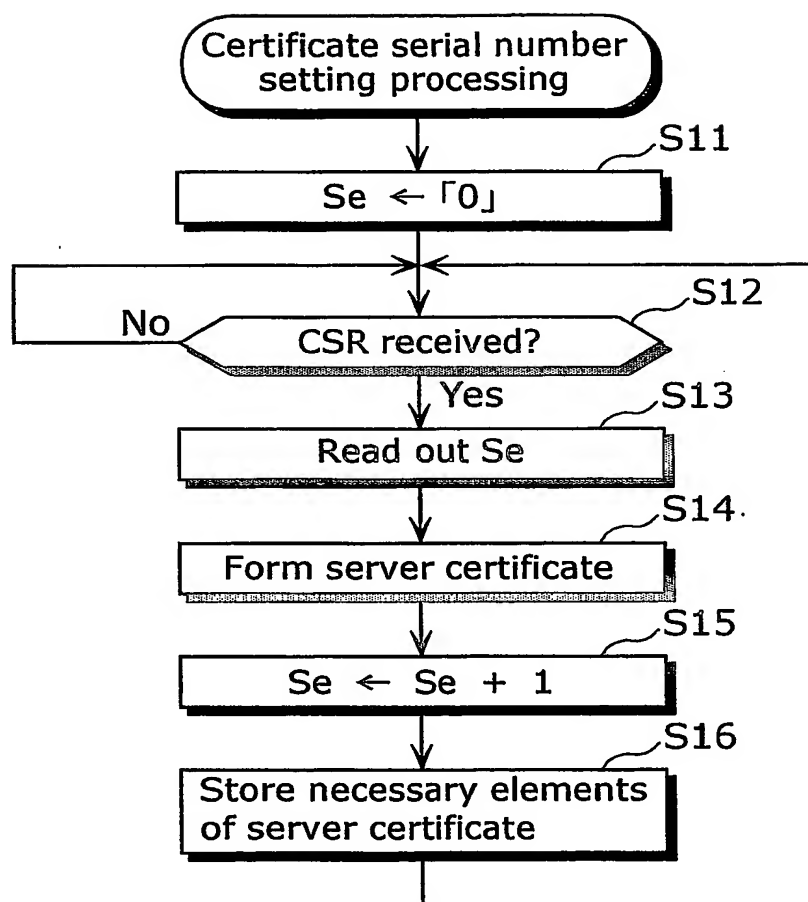


FIG. 12

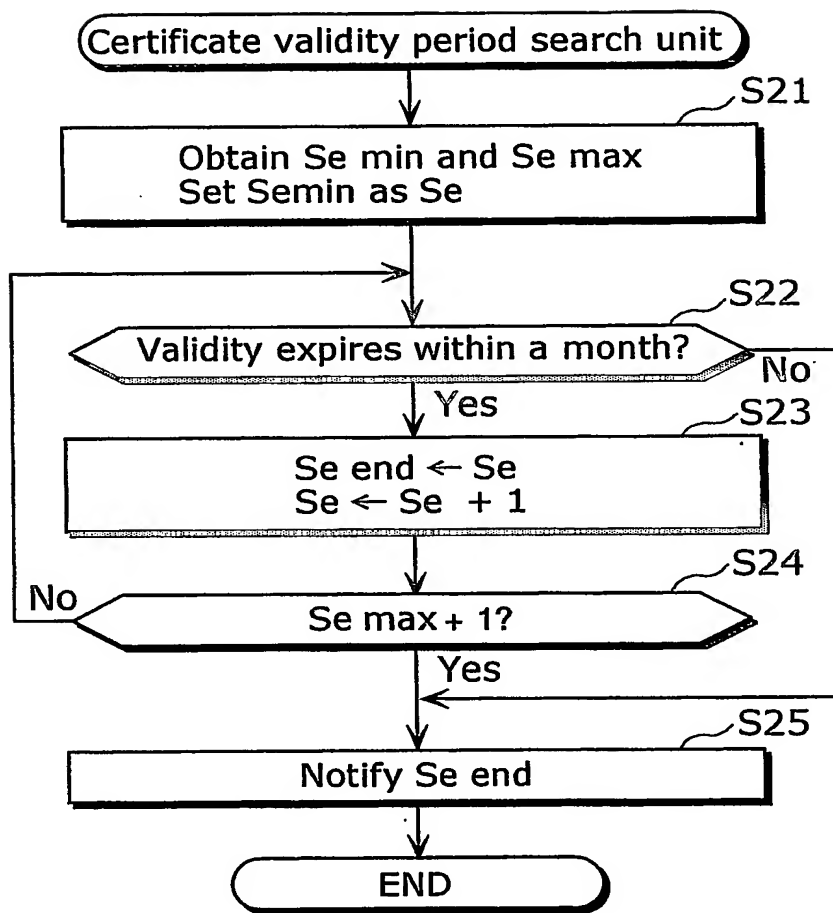


FIG. 13

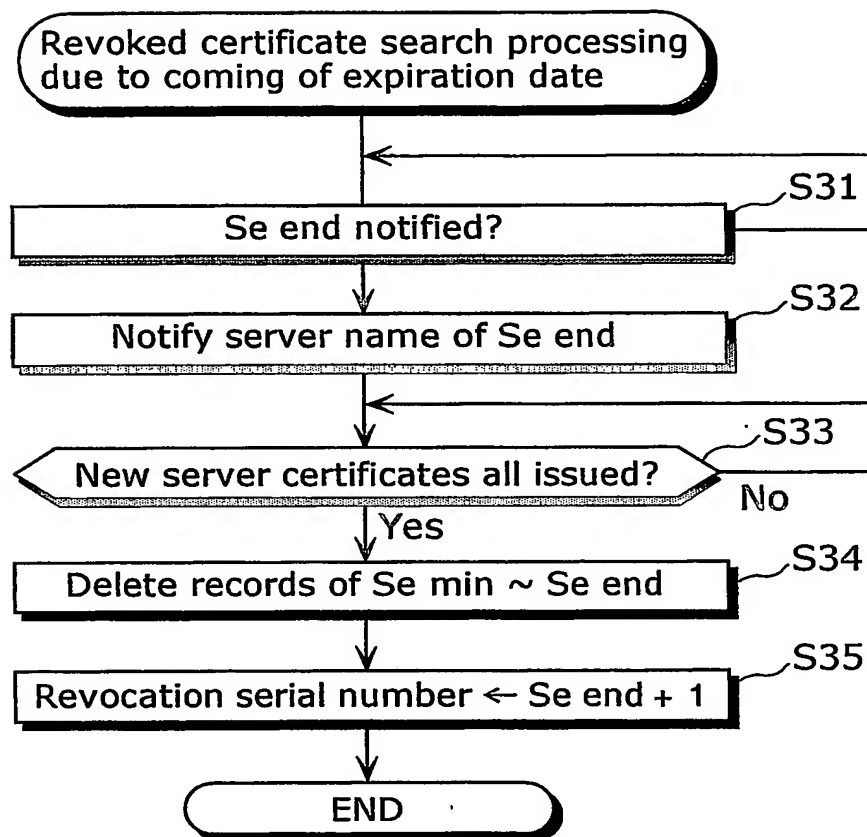


FIG. 14

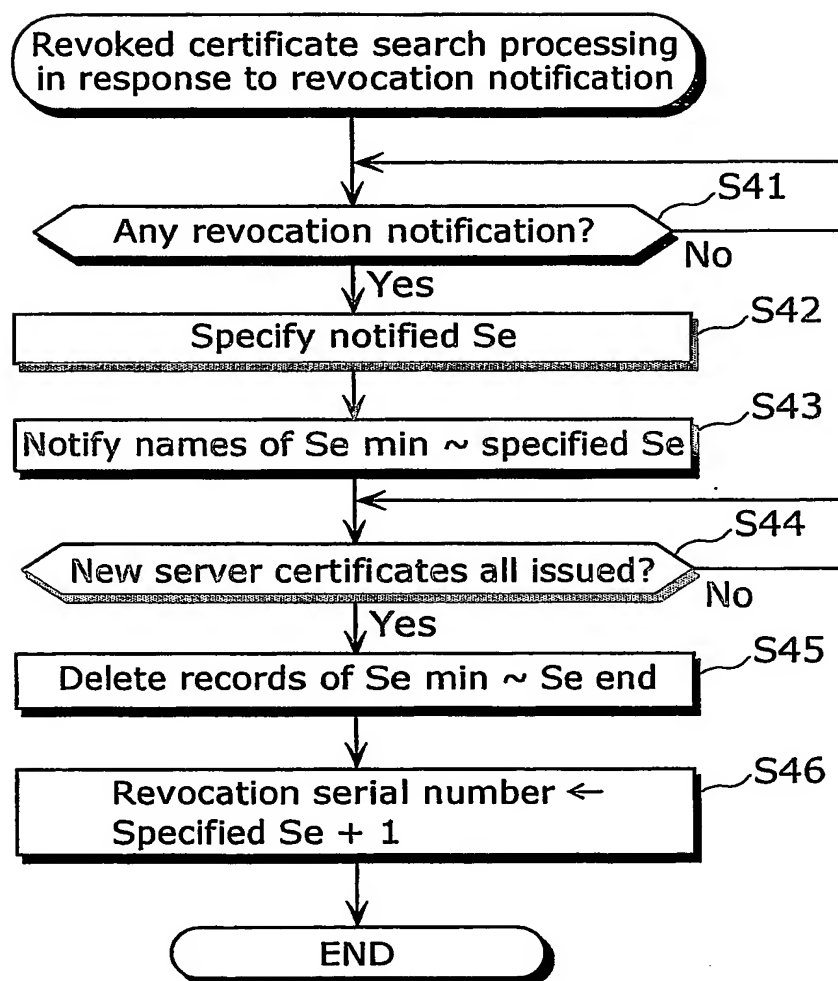


FIG. 15

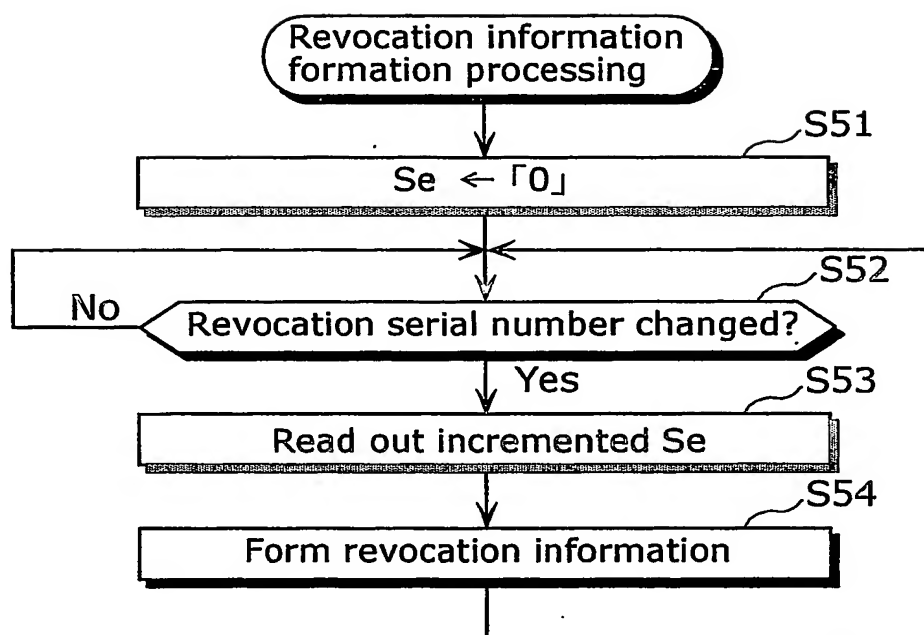
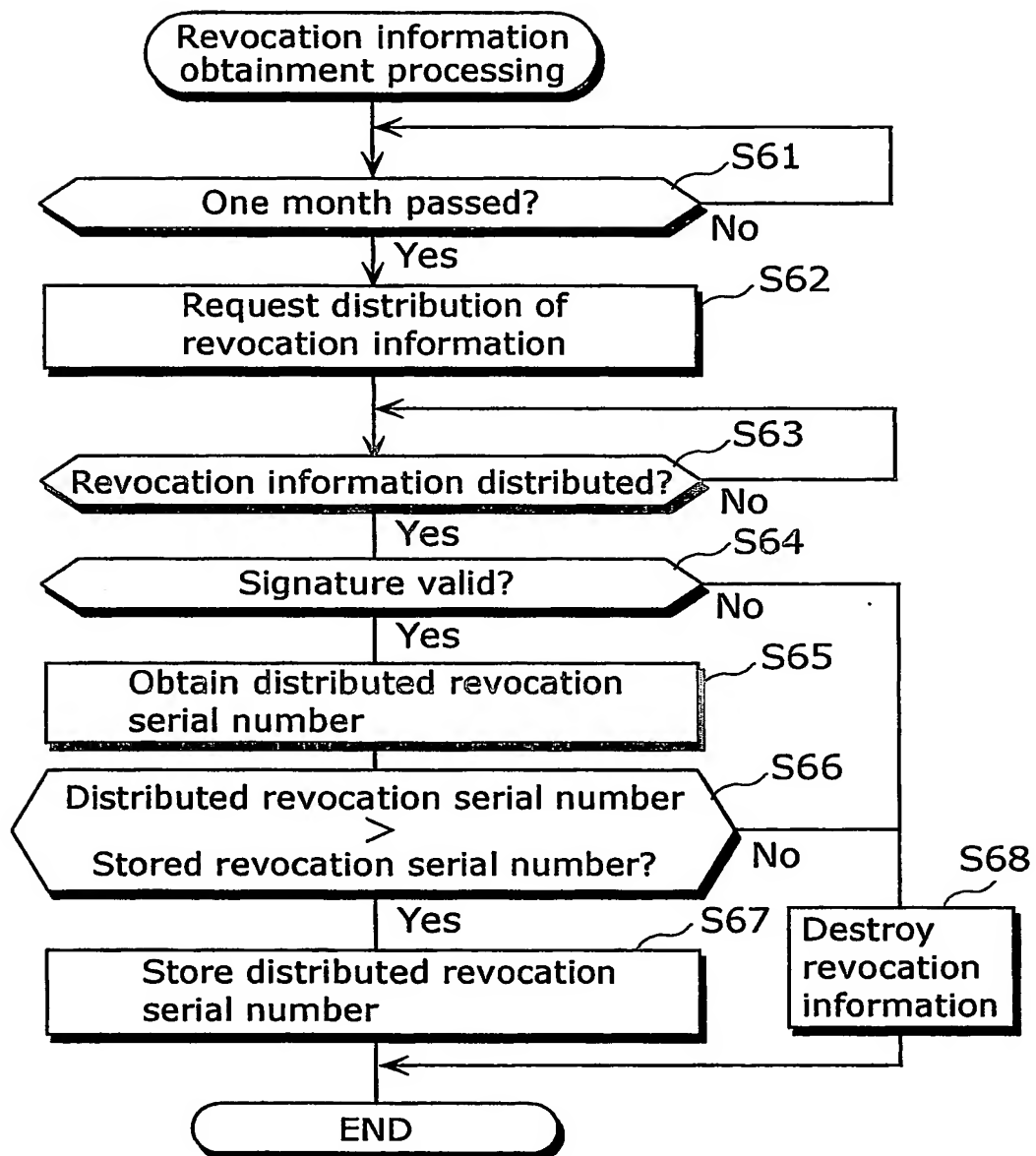


FIG. 16





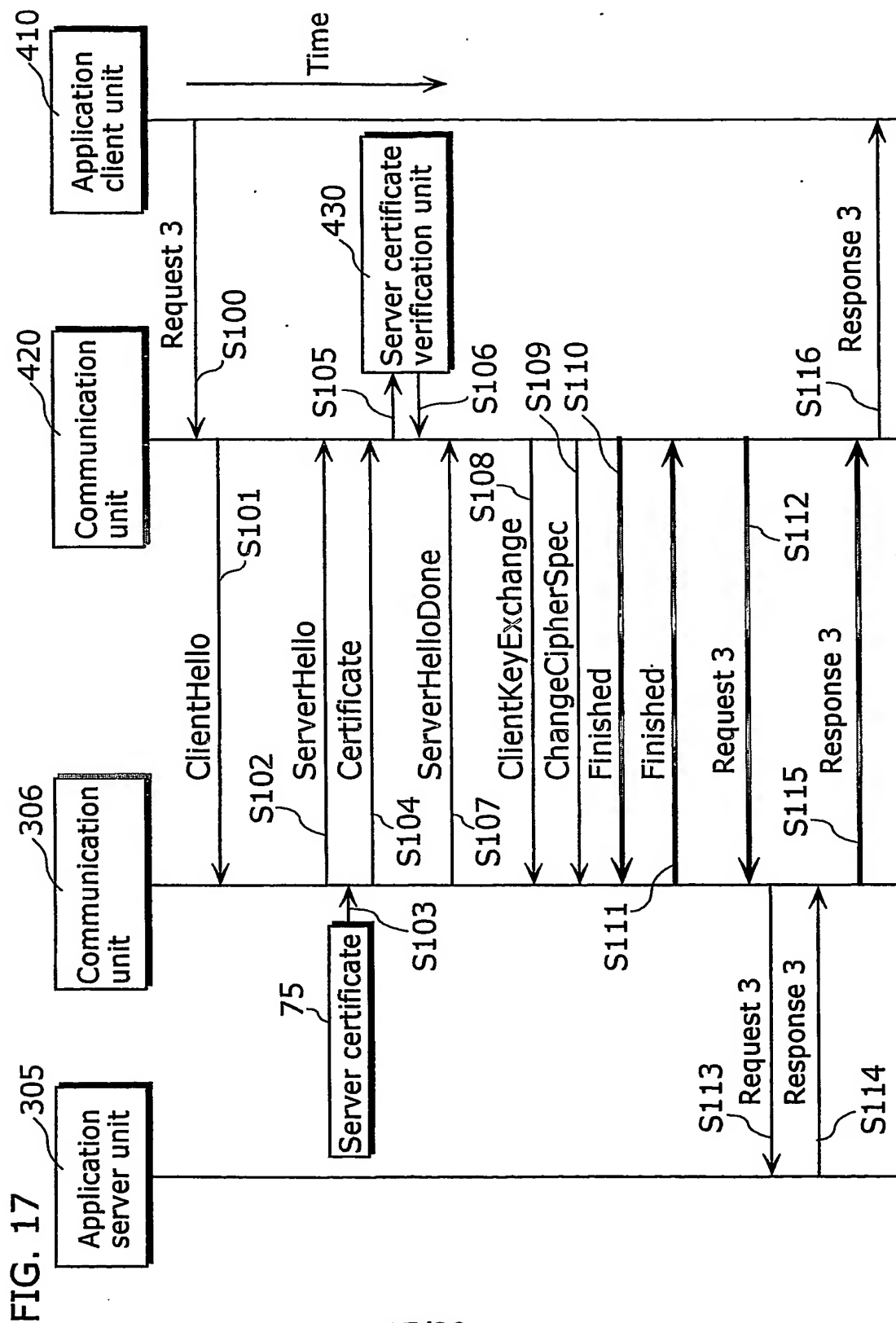


FIG. 18

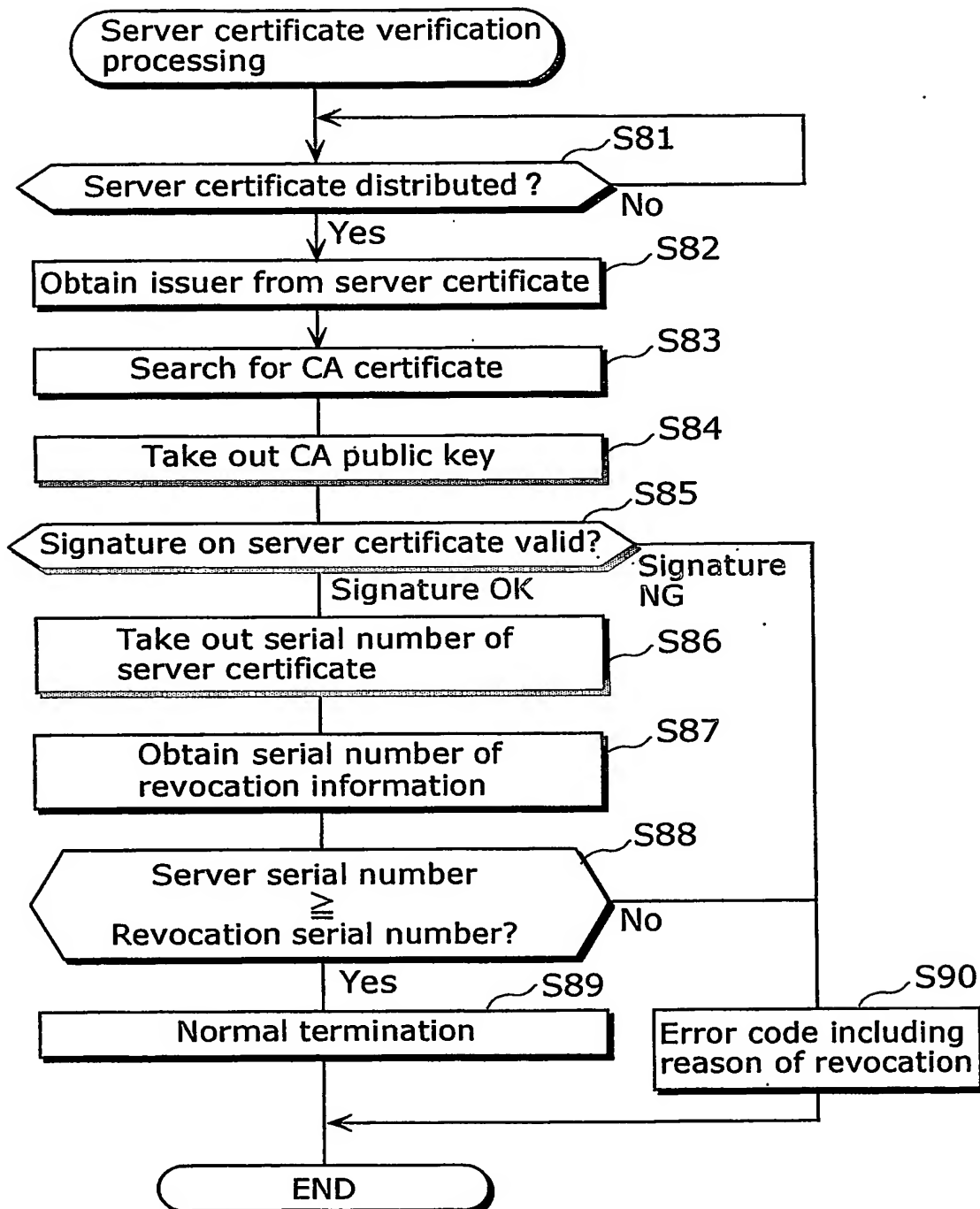


FIG. 19

	a	b	c	d	e	d+13	e+13
Server A				0		4	8
Server B				1		5	9
Server C				2		6	10
Server D					3		7
Revocation number				0		3	4
							11

